A3 Cancl.

$(H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$. S_1 is split into two w-bit words H_2 and L_2. S_2 is computed as being equal to $L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$. S_3 is computed as being equal to $S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$. And the residue is determined by comparing S_3 to 2^w. If $S_3 < 2^w$, then the residue equals S_2. If $S_3 \geq 2^w$, then the residue equals $S_3 - 2^w$.

B. In the Claims:

Please renumber the claims as follows:

A1-A11	:	1-11
B1-B5	:	12-16
C1-C3	:	17-19
D1-D2	:	20-21
E1-E10	:	22-31

Please cancel claims 1-6 (A1-A6), 12-16 (B1-B5), and 22-25 (E1-E4), without prejudice.

Please amend the claims without prejudice as indicated below. A marked up copy of the amended claims showing insertions and deletions is attached to this Response in Appendix A.

7. (Amended) A method of encrypting data comprising:

performing a ring arithmetic function on numbers, including:

using a residue number multiplication process;

converting to a first basis using a mixed radix system;

converting to a second basis using a mixed radix system;

choosing a modulus C for modular calculations;

wherein the modulus C is w-big; and

wherein the modulus C is w-heavy.

A4

8. (Amended) The method of claim 7,

wherein the modulus C is of the form $2^w - L$; and

wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$.

9. (Amended) The method of claim 8, further comprising:

calculating the modulus C by a process including:

splitting P into 2 w-bit words H_1 and L_1;

A4 calculating $S_1 = L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$;

splitting S_1 into two w-bit words H_2 and L_2;

computing $S_2 = L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$;

computing $S_3 = S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$;

determining the modulus C by comparing S_3 to 2^w, wherein the modulus $C = S_2$ if $S_3 < 2^w$, and wherein the modulus $C = S_3 - 2^w$ if $S_3 \geq 2^w$; and

wherein the modulus C is a residue.

10. (Amended) A method of encrypting data comprising:

performing a ring arithmetic function on numbers, including:

using a residue number multiplication process;

converting to a first basis using a mixed radix system;

converting to a second basis using a mixed radix system;

choosing a modulus C for modular calculations;

wherein the modulus C is w-little; and

wherein the modulus C is w-light.

A4 cancl. 11. (Amended) The method of claim 10,

wherein the modulus C is of the form $2^w + L$; and

wherein the modulus C has a Hamming weight close to 1.

18. (Amended) The method of claim 17,

wherein the modulus C is of the form $2^w - L$; and

wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$.

19. (Amended) The method of claim 18, further comprising:

A5 calculating the modulus C by a process including:

splitting P into 2 w-bit words H_1 and L_1;

calculating $S_1 = L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$;

splitting S_1 into two w-bit words H_2 and L_2;

computing $S_2 = L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$;

computing $S_3 = S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$;

determining the modulus C by comparing S_3 to 2^w, wherein the modulus $C = S_2$ if $S_3 < 2^w$, and wherein the modulus $C = S_3 - 2^w$ if $S_3 \geq 2^w$; and

wherein the modulus C is a residue.

21. (Amended) The method of claim 20,

A6 wherein the modulus C is of the form $2^w + L$; and

A6 cont.

wherein the modulus C has a Hamming weight close to 1.

26. (Amended) A method of hashing data comprising:

performing a ring arithmetic function on numbers, including:

using a residue number multiplication process;

converting to a first basis using a mixed radix system;

converting to a second basis using a mixed radix system;

A7

choosing a modulus C for modular calculations;

wherein the modulus C is w-big; and

wherein the modulus C is w-heavy.

27. (Amended) The method of claim 26,

wherein the modulus C is of the form $2^w - L$; and

wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$.

28. (Amended) The method of claim 27, further comprising

calculating the modulus C by a process including:

splitting P into 2 w-bit words H_1 and L_1;

calculating $S_1 = L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$;

splitting S_1 into two w-bit words H_2 and L_2;

computing $S_2 = L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$;

computing $S_3 = S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$;

determining the modulus C by comparing S_3 to 2^w, wherein the modulus $C = S_2$ if $S_3 < 2^w$, and wherein the modulus $C = S_3 - 2^w$ if $S_3 \geq 2^w$; and

wherein the modulus C is a residue.

29. (Amended) The method of Claim 28, wherein the method of hashing data comprises a method of cryptographic hashing.

30. (Amended) A method of hashing data comprising:

#7 Cond.

performing a ring arithmetic function on numbers, including:

using a residue number multiplication process;

converting to a first basis using a mixed radix system;

converting to a second basis using a mixed radix system;

choosing a modulus C for modular calculations;

wherein the modulus C is w-little; and

wherein the modulus C is w-light.

31. (Amended) The method of claim 30,

wherein the modulus C is of the form $2^w + L$; and

wherein the modulus C has a Hamming weight close to 1.